REMARKS

Claims 71-80 are pending. Claims 71-74, 79 and 80 have amended herein. No new claims have been added.

Allowable Claims:

The Applicant appreciates the Examiner's identification of allowable subject matter at items 11 and 12 of the Office Action. Claims 73 and 74 have been amended above to place them into independent form, incorporating the limitations of their respective base claims, in order to place claims 73-78 into condition for allowance. Only claims 71, 72, 79 and 80 remain rejected over the prior art.

Drawings:

Item 2 on page 2 of the Office Action requested drawings to be provided for showing the steps of encrypting, decrypting, and re-encrypting the data, and other features recited in claims 71-80. Accordingly, a change to Fig. 10 and a new drawing Fig. 11 are submitted in the enclosed Request for Approval of Drawing Changes. Corresponding descriptions were added to the specification by this amendment. The Applicant submits that no new matter was added.

Rejections under 35 U.S.C. §112, second paragraph:

Claims 71-74, 79, and 80 were rejected under 35 U.S.C. §112, second paragraph. Claims 71-74 were amended above to correct the phrase "and/or" to -- or --. In addition, claims 79 and 80 were amended above to provide the proper antecedent basis for "copyright information" in

the body of said claims. Accordingly, all the claims meet the requirements under 35 U.S.C. §112.

Rejections under 35 U.S.C. §103:

Claims 71, 72, 79, and 80 were rejected under 35 U.S.C. §103 over **Matsumoto et al.** (U.S. Patent No. 5,465,299) in view of **Shanton** (U.S. Patent No.5,369,702). It is submitted that nothing in the prior art, either alone or in combination, teaches or suggests all the features recited in the present claimed invention.

With regard to **Matsumoto et al.** the Office Action identifies portions thereof allegedly disclosing the encryption of unencrypted data using a first secret key of a first user, supplying the encrypted data to a second user, decrypting the encrypted data using the **public key** of the first user, displaying the decrypted data, re-encrypting the decrypted data using a second secret key, and storing, copying, or transferring the re-encrypted data. As described in the Office Action, **Matsumoto et al.** does not disclose decryption using the same key that was used to encrypt the data in the first place. Apparently, the Office Action makes the further reference to **Shanton** for disclosing the use the same secret key for encryption by a first user and decryption by a second user.

There appears to be some misunderstanding in the Office Action with regard to the disclosures of **Matsumoto et al.** In **Matsumoto et al.**, the secret key is used to make a digital signature. Such digital signatures are used in an asymmetric key system and not in a symmetric key system. Such secret keys used in digital signatures do not correspond to the "secret key" recited in claims 71 and 72. Instead, the "secret key" disclosed in **Matsumoto et al.** corresponds

to a "private key" described in the bottom six lines on page 11 of the present specification. Although **Matsumoto et al.** discloses the use of a "secret key" or a "private key" for use in making a digital signature, encryption and decryption are performed through a conventional asymmetric, public/private key system.

A crypt key system primarily includes a symmetric key system and an asymmetric key system. The symmetric key system uses the same key for both the encryption and decryption, and is commonly referred to as a "common key system" because of the use of a common key for encryption and decryption, or alternatively referred to as a "secret key system" because of the use of keys that are to be secret. The asymmetric key system uses different keys for encryption and decryption. One key (which is open to the public) is called a "public key" and other key (which is not publically available) is called a "private key" or a "secret key." As can be appreciated, the use of the term "secret key" may be used to refer to different types of keys in different types of key systems.

To one of ordinary skill in the art at the time of the invention, the use of a public/private key system for encryption and decryption (such as that described in **Matsumoto et al.**) is not combined with the common key system (such as that disclosed in **Shanton**). In the conventional common key system (like that disclosed in **Shanton**), there is no motivation to use a different second secret key for re-encryption. For at least these reasons, the present claimed invention patentably distinguishes over the prior art.

In addition, the information or data that is encrypted according to the disclosures of **Matsumoto et al.** is not "copyrighted data" as recited in amended claim 71. Instead, the information that is encrypted or decrypted according to the disclosures of **Matsumoto et al.** are

version management information or hash total of document data (not the copyrighted content itself that is to be displayed/performed or edited). For at least these further reasons, the present claimed invention patentably distinguishes over the prior art.

Moreover, nothing in the cited prior art teaches or suggests storing, copying, or transferring *only* the re-encrypted data (claim 71) or the encrypted edited data (claim 72) (i.e., **not the decrypted versions thereof**). The requirement to store, copy, or transfer only encrypted versions of data achieves a primary feature of the present invention to maintain a robust copyright protection management method. For at least these further reasons, the present claimed invention patentably distinguishes over the prior art.

Double Patenting:

Claims 71-80 were rejected under the judicially created doctrine of obviousness-type double patenting over claims 1-4 of U.S. Patent No. 6,069,952. These rejections are rendered moot in view of the enclosed Terminal Disclaimer.

Summary:

It is believed that the claims, as amended, contain patentable subject matter, and are now in condition for allowance. Should the Examiner deem that any further action by Applicants would be desirable to place the application in better condition for allowance, the Examiner is encouraged to telephone Applicant's undersigned attorney.

Attached herewith is a paper showing the claims, as amended, and entitled "VERSION WITH MARKINGS TO SHOW CHANGES MADE."

In the event that this paper is not timely filed, Applicant respectfully petitions for an appropriate extension of time. The fees for such an extension or any other fees which may be due with respect to this paper, may be charged to Deposit Account No. 01-2340.

Respectfully submitted,

ARMSTRONG, WESTERMAN, HATTORI,
McLELAND & NAUGHTON, LLP

John P. Kong
Attorney for Applicant(s)
Registration No. 40,054

Attorney Docket No. **990696A**
1725 K Street, N.W., Suite 1000
Washington, D.C. 20006
Tel: (202) 659-2930
JPK/sdj

Enclosures: Version with Markings to Show Changes Made
Petition for Extension of Time
Submission of Terminal Disclaimer
Request for Approval of Drawing Changes

VERSION WITH MARKINGS TO SHOW CHANGES MADE
U.S. Serial No. 09/476,334

IN THE SPECIFICATION:

On page 10, after line 4, the following paragraph has been inserted:

-- Figure 11 generally describes a data copyright management system of the present invention.--

On page 129, after line 16, the following paragraph has been inserted:

--As described in detail above, and generally shown in Fig. 11, a user decrypts encrypted data (encrypted with a first secret key) using the first secret key. The decrypted data is re-encrypted with a second secret key before the user can store, copy, or transfer it. The decrypted data may be displayed or edited. If edited, the edited data is encrypted with the second secret key before the user can store, copy, or transfer it. These operations of decryption, re-encryption, and encryption on the user's side are performed by a copyright control program. Copyright information may be added to the unencrypted data, encrypted data, decrypted data, and re-encrypted data for further copyright control and tracking.--

IN THE CLAIMS:

71. (Amended) A data copyright management method for managing the copyright of data ~~wherein a first secret key and a second secret key are used~~, ~~said method~~ comprising ~~the steps of~~:

encrypting unencrypted copyrighted data using ~~said~~ a first secret-key;

supplying the encrypted data to a primary user;

decrypting the encrypted data using said first secret-key;

displaying the decrypted data;

re-encrypting said decrypted data using ~~said~~ a second secret-key; and

storing, copying ~~and~~/or transferring said re-encrypted data and not said decrypted data.

72. (Amended) A data copyright management method according to claim 71, further comprising ~~the steps of~~:

editing said decrypted data to produce unencrypted edited data;

encrypting the unencrypted edited data using said second secret-key;

storing ~~the encrypted edited data~~, copying ~~said encrypted edited data and~~/ or transferring said encrypted edited data ~~to a secondary user~~ and not the unencrypted edited data.

73. (Amended) A data copyright management method, ~~according to claim 71, said method further using a copyright control program and~~ comprising ~~the step of~~:

encrypting unencrypted data using a first secret-key;

supplying the encrypted data to a primary user;

decrypting the encrypted data using said first secret-key;

displaying the decrypted data;

re-encrypting said decrypted data using a second secret-key; and

storing, copying or transferring said re-encrypted data,

~~carrying out~~ wherein at least one of said decrypting and~~/or~~ re-encrypting steps ~~by said~~ is carried out using a copyright control program.

74. (Amended) A data copyright management method, ~~according to claim 72, said method further using a copyright control program and~~ comprising ~~the step of~~:

encrypting unencrypted data using a first secret-key;

supplying the encrypted data to a primary user;

decrypting the encrypted data using said first secret-key;

displaying the decrypted data;

re-encrypting said decrypted data using a second secret-key;

editing said decrypted data to produce unencrypted edited data;

encrypting the unencrypted edited data using said second secret-key;

storing, copying or transferring said re-encrypted data; and

storing, copying or transferring said encrypted edited data,

~~carrying out~~ wherein at least one of said decrypting and~~/or~~ encrypting steps ~~by said~~ is carried out by a copyright control program.

75. (Amended) A data copyright management method according to claim 73, further comprising ~~the step of~~ pre-storing said copyright control program in a ROM of a user terminal used by said primary user and said secondary user.

VERSION WITH MARKINGS TO SHOW CHANGES MADE
U.S. Serial No. 09/476,334

76. (Amended) A data copyright management method according to claim 74, further comprising ~~the step of~~ pre-storing said copyright control program in a ROM of a user terminal used by said primary user and said secondary user.

77. (Amended) A data copyright management method according to claim 73, further comprising ~~the step of~~ pre-storing said copyright control program in an area managed by an operating system of a user terminal used by said primary user and said secondary user.

78. (Amended) A data copyright management method according to claim 74, further comprising ~~the step of~~ pre-storing said copyright control program in an area managed by an operating system of a user terminal used by said primary user and said secondary user.

79. (Amended) A data copyright management method according to claim 71, ~~said method~~ further ~~using copyright information and~~ comprising ~~the step of~~: adding ~~said~~ copyright information to said unencrypted data, said encrypted data, said decrypted data and said re-encrypted data.

80. (Amended) A data copyright management method according to claim 72, ~~said method~~ further ~~using copyright information and~~ comprising ~~the step of~~: adding ~~said~~ copyright information to said encrypted edited data.